

UNITED STATES DISTRICT COURT

for the
Northern District of Texas

FILED

NOV 18 2016

CLERK, U.S. DISTRICT COURT

By Deputy

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)
Items a. thru p. described in Attachment A

Case No. 4:16-MJ-740

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A.

located in the Northern District of Texas, there is now concealed (identify the person or describe the property to be seized):

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
18 U.S.C. § 922(g)(1) and	Felon in Possession of a Firearm
26 U.S.C. § 5861(d)	

The application is based on these facts:

See attached Affidavit.

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.



Applicant's signature

P. Williams, ATF Special Agent

Printed name and title

Sworn to before me and signed in my presence.

Date: 11/18/16

City and state: Fort Worth, Texas



Judge's signature

Jeffrey L. Cureton, U.S. Magistrate Judge

Printed name and title

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT**

I, P. Williams, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit under Rule 41, Federal Rules of Criminal Procedure, in support of an application for a search warrant authorizing the seizure and forensic examination of three cellular telephones and other electronic devices, as described in Attachment A. These items were possessed by Justin Carroll JACK, on October 28, 2016, in the Northern Judicial District of Texas.

2. Affiant is employed by the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF), specifically as a Special Agent (SA) and has been so since January of 2016. Affiant is currently assigned to ATF's Dallas Field Division, specifically its Fort Worth Field Office. Prior to engaging in this employment, Affiant was a Uniformed Division Officer with the United States Secret Service for nearly 4 years. In 2016, at the Federal Law Enforcement Training Center, Affiant completed the Criminal Investigator Training Program and the ATF Special Agent Basic Training program. As a law enforcement officer, Affiant has training and experience in a variety of investigative methods relating to firearms involved crimes, to include but not limited to visual surveillance, electronic surveillance, investigative subject interviews, and use of arrest warrants.

3. Affiant has been assigned numerous investigations involving firearm activities and firearm offenses, which resulted in seizures of firearms, gun parts, and

ammunition. Affiant's investigations and participation in investigations conducted by other law enforcement officers, has kept Affiant in close contact with patterns and methods of operations of persons who violate the Federal Firearm laws.

4. Based on Affiant's training and experience, as well as based upon interviews with defendants, informants, and other witnesses and participants in the firearm- related criminal activity, Affiant is familiar with ways that individuals who possess, acquire or maintain firearms, whether prohibited or not, employ electronic communication via text message, email, internet, and social media to facilitate certain activities.

5. Affiant also knows that subjects engaged in firearm offenses often have evidence of such offenses on their cell phones, such as, but not limited to: photographs and videos displaying the subject in possession of firearms, as well as text messages, emails, and records showing the illegal purchase, possession, transfer, and sale of firearms. Individuals involved in firearms offenses commonly use cellular telephones to transmit and receive information via voice calls, text messages, e-mail, and direct-connect capabilities in furtherance of their firearm offenses. It is common for individuals involved with firearm offenses to store, electronically, on their cellular telephones: (1) contact lists; (2) records of sent and received voice calls; (3) records of sent and received text messages; (4) records of sent and received direct-connect calls; (5) records of sent and received e-mails; and (6) records of sent and received photographs and videos. This information often contains evidence of firearm offenses, including evidence of the illegal purchase, possession, sale, transfer or illegal modification of a firearm(s).

6. Furthermore, Affiant knows that individuals engaged in firearms offenses often have evidence of such actions maintained within the content of electronic mediums, such as, but not limited to, hard drives, computer towers, laptops, and electronic storage devices (SD cards, thumb drives, and flash drives). These electronic mediums are often utilized in furtherance of committing firearm related offenses as well, to include, but not limited, to the unlawful purchase of firearm(s) and ammunition, as well as programs designed to unlawfully manufacture firearms. Moreover, these devices often store information germane to the aforementioned offenses, for example electronic receipts, internet browsing histories, videos, photographs, and emails.

7. The facts in this affidavit are the product of Affiant personal observations, training and experience, as well as information obtained from other law enforcement officers, and witnesses. This affidavit is intended to show that there is sufficient probable cause for the requested warrant and does not set forth all of the Affiant's knowledge or all of the information about this matter. Based on Affiant's training, experience, and the facts set forth in this affidavit, there is probable cause to believe that Justin Carroll JACK has violated the following statutes:

- a. Title 18, U.S.C., § 922 (g)(1) - It shall be unlawful for any person who has been convicted in any court of, a crime punishable by imprisonment for a term exceeding one year; to ship or transport in interstate or foreign commerce, or possess in or affecting commerce, any firearm or ammunition; or to receive any firearm or ammunition which has been shipped or transported in interstate or foreign commerce.

- b. Title 26, U.S.C., § 5861 (d) – It shall be unlawful for any person to receive or possess an National Firearms Act firearm not registered to that individual in the National Firearm Registration and Trade Record.

There is also probable cause to search the information described in Attachment A for evidence of these crimes as described in Attachment B.

PROBABLE CAUSE

8. On or October 27, 2016, Affiant was contacted, via telephone, by Wise County Sheriff's Office Detective J. Mayo, in reference to incident/offense report 16-099997, which was completed on October 26, 2016. The report was regarding an individual converting semi-automatic lower rifle receivers into fully automatic lower rifle receivers, as well as using an oil filter as a suppressor. Affiant was also informed by Detective Mayo that the individual unlawfully possessed firearms.

9. On that same day, Affiant was provided with a copy of the aforementioned incident/offense report, which indicated that the individual suspected of engaging in the listed activity was Justin Carroll JACK (W/M; YOB: 1977). In the report, a Cooperating Witness (CW) detailed JACK's engagement in the aforementioned activities. The CW also provided photographs of a suspected automatic lower rifle receiver, a fitting (used to convert an oil filter into a suppressor) and an attached oil filter, as well as a cache of firearms located throughout JACK's residence, to include within JACK's bedroom. Shortly thereafter, Affiant reviewed JACK's criminal history and determined that JACK had been previously convicted of felony offenses within Dallas County, Texas.

10. On October 27, 2016, Affiant obtained a federal search warrant for the residence of JACK, due the existence of probable cause that JACK unlawfully possessed firearms.

11. On October 28, 2016, at approximately 7:30 am, ATF and the Wise County Sheriff's Office (WCSO) executed a federal search warrant on the residence of JACK, located at 1221 County Road 1180, Decatur, Texas, 76234. During the execution of the search warrant, WCSO Deputies located JACK in his bedroom, on the left side of the bed. At that time, JACK was detained by the Sheriff's Deputies, then escorted outside of his residence. Also, present at the home was the CW. Later on that morning, JACK's wife, Heather Jack (W/F; YOB: 1980) arrived at the residence as well.

12. The search warrant yielded the discovery and seizure of seventeen (17) firearms, one suspected (1) automatic lower rifle receiver, and (1) fitting and oil filter used as a suppressor, both of which are National Firearms Act (NFA) firearms that are required to be registered with the National Firearms Registration and Transfer Record (NFRTR). Subsequently, Affiant queried the NFRTR for JACK's registration corresponding to the listed items, as well as any other NFA weapons, however found that JACK was not of any record with the NFRTR. The search warrant also led to the discovery and subsequent retention for evidence of a number of electronic mediums, to wit: (1) Apple cellular telephone, model: A1634, IMEI: 355728072184812, (1) Samsung cellular telephone, model: SM-N910A, SN: R38FB0VZGAR, IMEI: 356204063017501, (1) HP laptop, model 15-W105WM, SN: 8CG6193B5J, P/N: XOS29UA#ABA, (1) ASUS Computer, model: M51AC-B07, SN: DAPDCG0008BJ, (1) Wireless Adaptor

(Thumb Drive), Model Cechya-0082, SN: 215062002004, (1) Black and silver flash drive, model: N/A, SN: N/A, (1) Kingston Technology SD Card, N0105-001.AOOLF, 3729543, JM94174-941.AOOLF, (1) Philips Respironics, Recorders: 1054462, MMAGF02GWMCU-PA, TC00100938, (1) Sandisk 64GB Microsd Card and Sandisk Microsd Adapter, SN: 6246PRA45289, (1) Hard drive SN: WXCY08J53248, (1) Hard drive SN: 9VP1KMHX, (1) Hard drive SN: 5JXHQPV8, (1) Hard drive SN: IH8X06, (1) Hard drive SN: T306512, (1) Hard drive SN: 604IFOMMS.

13. Further into the search of the JACK residence, the CW led ATF Agents and WCSO Deputies to a gun firing range located on the premise, which contained a large number of spent ammunition shell casings. At that time, the CW indicated that JACK purchases large quantities of ammunition, via the internet. In concurrence, during the execution of the search warrant at the JACK residence, a Cheaper Than Dirt! Shooting Sports Discounter invoice was located and retained for evidence, which was specifically addressed to JACK. The invoice displayed the purchase of "RWS 22LR Subsonic 40GR" ammunition.

14. Also, during ATF's time at the JACK residence, an interview of Heather Jack was completed by ATF SA M. Finney, at which time Heather Jack indicated that there were images and videos of JACK shooting firearms on her cellular telephone. Heather Jack further indicated that JACK sent her the images and videos from his cellular telephone. Ultimately, Heather Jack provided consent for the search of her cellular telephone. Further into the listed interview, Heather Jack opined that her laptop, which was retained for evidence by ATF, contained a program that JACK used to enabled the

CNC machine (Ghost Gunner Machine) to function, moreover convert semi-automatic lower rifle receivers to fully automatic lower rifle receivers. Heather also stated that JACK ordered ammunition, via the internet, through JACK's work computer, which was also retained for evidence by ATF.

15. Then, on that same day, the CW asserted to ATF SA's that JACK had provided another individual with a firearm, specifically a Mark Goss. Shortly thereafter, Goss was interviewed, at his home, by ATF SA's and WCSO Deputies in an effort to further establish JACK's activities in relation to firearms. During that interview, Goss accessed his own Facebook social media page, then accessed JACK's Facebook social media page, which displayed videos and images of JACK possessing and shooting firearms.

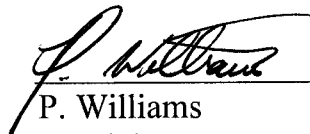
16. Later that same day, Heather Jack responded to the WCSO and provided ATF SA Finney with a cellular telephone that she asserted was JACK's old cellular telephone, to wit: (1) Apple cellular telephone, model: A1634, IMEI: 353294074623630.

CONCLUSION

17. Based on Affiant's knowledge and experience with firearms offenses, as well as informed by the facts and circumstances presented above, Affiant believes that probable cause exists that the forensic processing of the cellular telephones and electronic mediums described and explained in Attachment A contain: (1) evidence of the unlawful possession of firearms and ammunition; (2) evidence regarding the purchase of firearms; to include firearms not registered to JACK in the National Firearms Registration and Transfer Record (plans to sell or distribute them, and how, as well as under what

circumstance the weapons were acquired); (3) evidence showing that the cellular telephones were used or intended to be used to facilitate illegal activities; and (4) evidence of the fruits of illegal activities.

Respectfully submitted,



P. Williams
Special Agent
Bureau of Alcohol, Tobacco, Firearms and
Explosives

Sworn to before me and subscribed in my presence, November 18, 2016, in Fort Worth, Texas, at 2:01 p.m.



JEFFREY L. CURETON
United States Magistrate Judge

ATTACHMENT A

DESCRIPTION OF ITEMS TO BE SEARCHED

- a) Apple cellular telephone, model: A1634, IMEI: 353294074623630
- b) Apple cellular telephone, model: A1634, IMEI: 355728072184812
- c) HP laptop, model 15-W105WM, SN: 8CG6193B5J, P/N
XOS29UA#ABA
- d) Samsung cellular telephone, model: SM-N910A, SN: R38FB0VZGAR,
IMEI: 356204063017501
- e) Wireless Adaptor (Thumb Drive), Model Cechya-0082, SN:
215062002004
- f) Black and silver flash drive, model: N/A, SN: N/A
- g) ASUS Computer, model: M51AC-B07, SN: DAPDCG0008BJ
- h) Kingston Technology SD Card, N0105-001.AOOLF, 3729543,
JM94174-941.AOOLF
- i) Philips Respironics, Recorders: 1054462, MMAGF02GWMCU-PA,
TC00100938
- j) Sandisk 64GB MicroSD Card and Sandisk MicroSD Adapter, SN:
6246PRA45289
- k) Hard drive SN: WXCY08J53248
- l) Hard drive SN: 9VP1KMHX
- m) Hard drive SN: 5JXHQPV8
- n) Hard drive SN: IH8X06
- o) Hard drive SN: T306512
- p) Hard drive SN: 604IFOMMS

seized from Justin Carroll JACK and presently in ATF custody at 6000 Western Place,
Fort Worth, Texas 76107.

ATTACHMENT B

Conduct of forensic examination of items in Attachment A:

1. This warrant seeks authorization to examine all information contained on all the electronic mediums described in Attachment A, which relate to, facilitated, or contain evidence of a crime or fruits of a crime regarding violations of 18 U.S.C. § 922 (g)(1) and 26 U.S.C. § 5861(d) (possession of a firearm which is not registered to him in the National Firearms Registration), including:
 - a. All stored contacts, address books, calendar appointments;
 - b. Lists of customers and related identifying information;
 - c. All bank records, checks, credit card bills, account information, and other financial records;
 - d. Images or video used to promote or facilitate the illegal purchase and possession of firearms; and
 - e. Any locations or photos marked by Global Positioning Satellites (GPS) that are associated with the illegal activity.
2. Evidence of user attribution showing who used or owned the cellular phones, computers, storage mediums, and hard drives at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history.
3. Records evidencing the use of the Internet to communicate with others, including:
 - a. Records of Internet Protocol addresses used; and
 - b. Records of Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, records of user-typed web addresses, emails, text messaging, and phone call activity.

4. As used throughout this warrant, including in Attachments A and B, the terms:
- a. "Records" and "Information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form;
 - b. Wireless telephone or mobile telephone or cellular telephone is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.
 - c. Digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.
 - d. An Internet Protocol Address, or simply "IP address," is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP

addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

- e. The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

5. Based on my knowledge, training, and experience, I know that cellular phones, computers, storage mediums, and hard drives can store information for long periods of time. I also know that the cellular phones, computers, storage mediums, and hard drives described in Attachment A are capable of serving as a wireless telephone, digital camera, portable media player, GPS navigation device, and PDA, and are capable of storing various types of information such as call logs, text messaging, pictures and video, and personal contacts. In my training and experience, examining data stored on the cellular phones, computers, storage mediums, and hard drives described in Attachment A can uncover, among other things, evidence that reveals or suggests who possessed or used the device to facilitate the commission of an offense. Similarly, things that have been viewed via the Internet are typically stored for some period of time on devices. This information can sometimes be recovered with forensics tools.

7. Forensic evidence. This application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the cellular phones, computers, storage mediums, and hard drives were used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the cellular phones, computers, storage mediums, and hard drives because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file);
- b. Forensic evidence on a cellular phone, computers, storage mediums, and hard drives can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence;

- c. A person with appropriate familiarity with how cellular phones, computers, storage mediums, and hard drives work, after examining this forensic evidence in its proper context, may be able to draw conclusions about how the devices were used, the purpose of their use, who used them, and when;
 - d. The process of identifying the exact electronically stored information on cellular phones, computers, storage mediums, and hard drives that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data is stored on cellular phones, computers, storage mediums, and hard drives, evidence may depend on other information stored on the device or other devices and the application of knowledge about how the device behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant; and
 - e. In finding evidence of how electronic mediums were used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.
8. Nature of examination. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the electronic items described in Attachment A consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to, computer-assisted scans of the entire medium, which might expose many parts of the devices to human inspection to determine whether it is evidence described by the warrant.
9. Manner of execution. Because this warrant seeks only permission to examine electronic mediums already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.